

Distribution properties of compressing sequences derived from primitive sequences modulo odd prime powers

Yupeng Jiang and Dongdai Lin

State Key Laboratory Of Information Security,
Institute of Information Engineering,
Chinese Academy of Sciences, Beijing 100093, P.R. China
E-mail: {jiangyupeng, ddlin}@iie.ac.cn

Abstract

Let \underline{a} and \underline{b} be primitive sequences over $\mathbb{Z}/(p^e)$ with odd prime p and $e \geq 2$. For certain compressing maps, we consider the distribution properties of compressing sequences of \underline{a} and \underline{b} , and prove that $\underline{a} = \underline{b}$ if the compressing sequences are equal at the times t such that $\alpha(t) = k$, where $\underline{\alpha}$ is a sequence related to \underline{a} . We also discuss the s -uniform distribution property of compressing sequences. For some compressing maps, we have that there exist different primitive sequences such that the compressing sequences are s -uniform. We also discuss that compressing sequences can be s -uniform for how many elements s .

Keywords: Compressing map, integer residue ring, linear recurring sequence, primitive sequence, s -uniform.

1 Introduction

A sequence over a ring R is denoted by $\underline{a} = (a(t))_{t \geq 0}$ with each $a(t)$ belonging to R . Moreover, if there are elements c_0, c_1, \dots, c_{n-1} in R such that

$$a(i+n) = c_{n-1}a(i+n-1) + \dots + c_1a(i+1) + c_0a(i)$$

holds for all $i \geq 0$, then the sequence is called a linear recurring sequence of degree n over R , generated by $f(x) = x^n - c_{n-1}x^{n-1} - \dots - c_1x - c_0$.

Let p be a prime number, e a positive integer and $\mathbb{Z}/(p^e)$ the integer residue ring modulo p^e . We identify the elements of $\mathbb{Z}/(p^e)$ with the

corresponding representatives in $\{0, 1, 2, \dots, p^e - 1\}$. For two integers m and n , the notation $[n]_{\text{mod } m}$ represents the least nonnegative integer of n modulo m and $[\underline{a}]_{\text{mod } m} = ([a(t)]_{\text{mod } m})_{t \geq 0}$. These notations were used by Zheng, Qi and Tian in [13]. Then a recurring sequence over $\mathbb{Z}/(p^e)$ generated by $f(x) = x^n - c_{n-1}x^{n-1} - \dots - c_1x - c_0$ means that for all $i \geq 0$, $a(i) \in \{0, 1, 2, \dots, p^e - 1\}$ and

$$a(i+n) = [c_{n-1}a(i+n-1) + \dots + c_1a(i+1) + c_0a(i)]_{\text{mod } p^e}.$$

Usually, the set of all sequences generated by $f(x)$ over $\mathbb{Z}/(p^e)$ is denoted by $G(f(x), p^e)$.

Let $f(x)$ be a monic polynomial of degree n over $\mathbb{Z}/(p^e)$. If $[f(0)]_{\text{mod } p} \neq 0$, then there exists a positive integer T such that $x^T - 1$ is divisible by $f(x)$ in $\mathbb{Z}/(p^e)[x]$. The smallest such positive T is called the *least period* of $f(x)$ and denoted by $\text{per}(f(x), p^e)$. Ward proved that $\text{per}(f(x), p^e) \leq p^{e-1}(p^n - 1)$ [11]. Polynomials reaching this bound are called *primitive* polynomials. A sequence \underline{a} is called a *primitive* sequence of order n if \underline{a} is generated by a primitive polynomial of degree n and $[\underline{a}]_{\text{mod } p}$ is not the all zero sequence. It can be shown that primitive sequences of order n have least period $p^{e-1}(p^n - 1)$. For $e = 1$, primitive sequences are just the well known m-sequences over prime field $\mathbb{Z}/(p)$. The set of all primitive sequences generated by primitive polynomial $f(x)$ is usually denoted by $G'(f(x), p^e)$. More details of linear recurring sequences over integer residue rings can be found in [5].

Let $\underline{a} = (a(t))_{t \geq 0}$ be a sequence over $\mathbb{Z}/(p^e)$. Each $a(t)$ has a unique p -adic expansion as

$$a(t) = a_0(t) + a_1(t) \cdot p + \dots + a_{e-1}(t) \cdot p^{e-1},$$

with $a_i(t) \in \{0, 1, \dots, p-1\}$ for all $0 \leq i \leq e-1$. The sequence $\underline{a}_i = (a_i(t))_{t \geq 0}$ is called the *i th-level* sequence of \underline{a} , and

$$\underline{a} = \underline{a}_0 + \underline{a}_1 \cdot p + \dots + \underline{a}_{e-1} \cdot p^{e-1}$$

is called the p -adic expansion of \underline{a} .

Let $f(x)$ be a primitive polynomial over $\mathbb{Z}/(p^e)$ and $\phi(x_0, x_1, \dots, x_{e-1})$ be an e -variable polynomial over $\mathbb{Z}/(p)$. We can induce a map from the set of primitive sequences $G'(f(x), p^e)$ to the set of sequences over $\mathbb{Z}/(p)$ by the polynomial ϕ . The new map is also denoted by ϕ and defined by

$$\begin{aligned} \phi : G'(f(x), p^e) &\rightarrow (\mathbb{Z}/(p))^\infty \\ \underline{a} &\mapsto \phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1}) = (\phi(a_0(t), a_1(t), \dots, a_{e-1}(t)))_{t \geq 0}. \end{aligned}$$

The map ϕ is called a *compressing map* and $\phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1})$ is called a *compressing sequence*. $\phi(x_0, x_1, \dots, x_{e-1})$ is called an *injective function* if ϕ is injective.

Huang and Dai in [3, Theorem 1] and Kuzmin and Nechaev in [8, Theorem 2] independently proved that $\phi(x_0, x_1, \dots, x_{e-1}) = x_{e-1}$ is an injective function. Their result is presented as the following theorem.

Theorem 1. *Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$. For $\underline{a}, \underline{b} \in G'(f(x), p^e)$, $\underline{a} = \underline{b}$ if and only if $\underline{a}_{e-1} = \underline{b}_{e-1}$.*

The above theorem means that the sequence \underline{a}_{e-1} over $\mathbb{Z}/(p)$ contains all the information of the sequence \underline{a} over $\mathbb{Z}/(p^e)$. Theoretically, one can recover \underline{a} when given \underline{a}_{e-1} . The cryptographic properties of such compressing sequences have been studied in [1, 2, 6, 7]. From then on, more compressing maps have been proved to be injective. Especially, when $f(x)$ is a strongly primitive polynomial (Definition 2 in the next section), the following results are obtained for $p = 2$ and odd prime p respectively. For $p = 2$, Qi, Yang and Zhou [9] proved that almost all e -variable boolean functions containing x_{e-1} are injective. For odd prime p , the following theorem has been proved in [10, 14, 17].

Theorem 2. *Let $f(x)$ be a strongly primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with odd prime p and $e \geq 2$. Assume $g(x_{e-1}) \in \mathbb{Z}/(p)[x_{e-1}]$ with $1 \leq \deg g \leq p - 1$ and $\eta(x_0, x_1, \dots, x_{e-2}) \in \mathbb{Z}/(p)[x_0, x_1, \dots, x_{e-2}]$. Then the function*

$$\phi(x_0, x_1, \dots, x_{e-1}) = g(x_{e-1}) + \eta(x_0, x_1, \dots, x_{e-2})$$

is an injective function.

The distribution properties of compressing sequences are also interesting. Now we recall some definitions in [13].

Definition 1. Let $\underline{a} = (a(t))_{t \geq 0}$, $\underline{b} = (b(t))_{t \geq 0}$ and $\underline{c} = (c(t))_{t \geq 0}$ be three sequences over $\mathbb{Z}/(p)$, and let $s, k \in \mathbb{Z}/(p)$. Sequences \underline{a} and \underline{b} are called s -uniform, s -uniform with \underline{c} and s -uniform with $\underline{c}|_k$, respectively, if $a(t) = s$ iff $b(t) = s$ for all $t \geq 0$, for all $t \geq 0$ with $c(t) \neq 0$ and for all $t \geq 0$ with $c(t) = k$.

In [15] and [16], Zhu and Qi proved that when $e > 1$, $\underline{a} = \underline{b}$ iff \underline{a}_{e-1} and \underline{b}_{e-1} are 0-uniform. Later, the same authors [18] obtained a further result that $\underline{a} = \underline{b}$ iff \underline{a}_{e-1} and \underline{b}_{e-1} are 0-uniform with a certain sequence $\underline{\alpha}$ (definition given before Definition 2 in the next section). In [12], under

the condition that $f(x)$ is a strongly primitive polynomial, Zheng and Qi extended the result to the following more general one. Let

$$\phi(x_0, x_1, \dots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \dots, x_{e-2})$$

with the coefficient of $x_{e-2}^{p-1} \cdots x_1^{p-1} x_0^{p-1}$ in η is not equal to $(-1)^e \cdot \frac{p+1}{2}$. Then their result is $\underline{a} = \underline{b}$ if and only if there exist $s \in \mathbb{Z}/(p)$ such that $\phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1})$ and $\phi(\underline{b}_0, \underline{b}_1, \dots, \underline{b}_{e-1})$ are s -uniform with \underline{a} . Recently, the same author proved a stronger result [13] which is stated in the following.

Theorem 3. *Let $f(x)$ be a strongly primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with odd prime p and $e \geq 2$. Assume*

$$\phi(x_0, x_1, \dots, x_{e-1}) = x_{e-1} + \eta(x_0, x_1, \dots, x_{e-2})$$

with the coefficient of $x_{e-2}^{p-1} \cdots x_1^{p-1} x_0^{p-1}$ in η is not equal to $(-1)^e \cdot \frac{p+1}{2}$. Then for $\underline{a}, \underline{b} \in G'(f(x), p^e)$, $\underline{a} = \underline{b}$ if and only if there exist $s \in \mathbb{Z}/(p)$ and $k \in (\mathbb{Z}/(p))^$ such that $\phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1})$ and $\phi(\underline{b}_0, \underline{b}_1, \dots, \underline{b}_{e-1})$ are s -uniform with $\underline{a}|_k$.*

In this article, we will investigate that if x_{e-1} is replaced by a general polynomial $g(x_{e-1})$ in the above theorem, whether or not similar results can still hold. Unfortunately, the answer is negative. We obtain that if there exists $k \in (\mathbb{Z}/(p))^*$ such that $\phi(a_0(t), a_1(t), \dots, a_{e-1}(t)) = \phi(b_0(t), b_1(t), \dots, b_{e-1}(t))$ for all t satisfying $\alpha(t) = k$, then $\underline{a} = \underline{b}$. This result is stronger than Theorem 2, and we devote Section 3 to prove it. In Section 4, we consider that for some $g(x_{e-1})$ and different \underline{a} and \underline{b} , $\phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1})$ and $\phi(\underline{b}_0, \underline{b}_1, \dots, \underline{b}_{e-1})$ can be s -uniform for how many elements in $\mathbb{Z}/(p)$. In the next section, we recall some facts about primitive sequences modulo odd prime powers.

2 Preliminaries

In this section, we will introduce some facts about sequences over integer residue rings. we only consider the case that p is an odd prime.

For sequences $\underline{a} = (a(t))_{t \geq 0}$, $\underline{b} = (b(t))_{t \geq 0}$ over $\mathbb{Z}/(p^e)$, and $c \in \mathbb{Z}/(p^e)$, we have the following operation:

$$\underline{a} + \underline{b} = ([a(t) + b(t)]_{\text{mod } p^e})_{t \geq 0}, \quad c \cdot \underline{a} = ([c \cdot a(t)]_{\text{mod } p^e})_{t \geq 0},$$

$$x^k \underline{a} = (a(t+k))_{t \geq 0}.$$

Then the operation of a polynomial $g(x) = \sum_{k=0}^n c_k x^k \in \mathbb{Z}/(p^e)[x]$ on the sequence \underline{a} as

$$g(x)\underline{a} = \sum_{k=0}^n c_k \cdot x^k \underline{a}.$$

If $f(x)$ is a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$, it is known [3] that there exist polynomials $h_i(x)$ of degree less than n over $\mathbb{Z}/(p^e)$ such that for $1 \leq i \leq e$,

$$x^{p^{i-1}T} \equiv 1 + p^i \cdot h_i(x) \pmod{f(x)}, \quad (1)$$

where $T = p^n - 1$ and $h_1(x) \equiv h_2(x) \equiv \dots \equiv h_e(x) \not\equiv 0 \pmod{p}$. For a given $f(x)$, denote by $h_f(x)$ the polynomial of $h_1(x)$ modulo p . The sequence \underline{a} over $\mathbb{Z}/(p)$ mentioned in the last section is defined to be $[h_f(x)\underline{a}_0]_{\text{mod } p}$.

Definition 2. Let $f(x)$ be a primitive polynomial and $h_f(x) \equiv h_i(x) \pmod{p}$. If $h_f(x)$ is not constant, i.e., $\deg(h_f(x)) \geq 1$, then $f(x)$ is called a strongly primitive polynomial.

The following definition is given in [10]. It is used to deal with carries.

Definition 3. For $a = a_0 + a_1 \cdot p + \dots + a_{e-1} \cdot p^{e-1} \in \mathbb{Z}/(p^e)$, Define a function

$$\begin{aligned} C_1 : \quad \mathbb{Z}/(p^e) &\rightarrow \mathbb{Z}/(p) \\ a &\mapsto C_1(a) = a_1. \end{aligned}$$

For a sequence $\underline{a} = \underline{a}_0 + \underline{a}_1 \cdot p + \dots + \underline{a}_{e-1} \cdot p^{e-1}$ over $\mathbb{Z}/(p^e)$, Define $C_1(\underline{a}) = \underline{a}_1$.

For an element u in $\mathbb{Z}/(p) = \{0, 1, \dots, p-1\}$, the function C_1 can induce a map from $\mathbb{Z}/(p)$ to itself by $x \mapsto C_1(u+x)$. By Lagrange interpolation, each such function has a unique polynomial representation, and we have the following result [12].

Proposition 4. *The coefficient of x^{p-1} in the polynomial representation of the map $x \mapsto C_1(u+x)$ is $-u$.*

Let the equality (1) operates on a sequence \underline{a} generated by $f(x)$ over $\mathbb{Z}/(p^e)$. The following results can be proved. For details see [10] and [12].

Proposition 5. *Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$. Assume $\underline{a} \in G(f(x), p^e)$, $T = p^n - 1$, $h_i(x)$ and \underline{a} are defined as above. Then*

for integers $j \geq 0$, we have the following results.

(1) The equality

$$(x^{j \cdot p^{e-2}T} - 1)_{\underline{a}_{e-1}} \equiv j \cdot \underline{a} \pmod{p} \quad (2)$$

holds for $e \geq 2$.

(2) The equality

$$\begin{aligned} (x^{j \cdot p^{e-3}T} - 1)_{\underline{a}_{e-1}} &\equiv j \cdot (h_f(x)_{\underline{a}_1}) + C_1(j \cdot (h_{e-2}(x)_{\underline{a}_0}) + \\ &\quad C_1(\underline{a}_{e-2} + [j \cdot \underline{a}]_{\text{mod } p}) \pmod{p} \end{aligned} \quad (3)$$

holds for $e \geq 4$.

(3) The equality

$$\begin{aligned} (x^{j \cdot T} - 1)_{\underline{a}_2} &\equiv \binom{j}{2} h_f^2(x)_{\underline{a}_0} + j \cdot (h_f(x)_{\underline{a}_1}) + \\ &\quad C_1(j \cdot (h_1(x)_{\underline{a}_0}) + C_1(\underline{a}_1 + [j \cdot \underline{a}]_{\text{mod } p}) \pmod{p} \end{aligned} \quad (4)$$

holds.

The following statements about periods of linear recurring sequences over $\mathbb{Z}/(p^e)$ can be proved similarly as in [1].

Proposition 6. Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ and $\underline{a} \in G(f(x), p^e)$ have p -adic expansion $\underline{a} = \underline{a}_0 + \underline{a}_1 \cdot p + \cdots + \underline{a}_{e-1} \cdot p^{e-1}$. Assume $T = p^n - 1$. Then

- (1) if $\underline{a}_0 \neq \underline{0}$, then $\text{per}(\underline{a}_i) = p^i T$ for $0 \leq i \leq e-1$ and $\text{per}(\underline{a}) = p^{e-1} T$,
- (2) if $\underline{a}_0 = \underline{a}_1 = \cdots = \underline{a}_{i-1} = \underline{0}$ and $\underline{a}_i \neq \underline{0}$ for $0 \leq i \leq e-1$, then $\text{per}(\underline{a}) = p^{e-1-i} T$.

For m -sequences over $\mathbb{Z}/(p)$, The following results are well known.

Proposition 7. Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p)$, and $\underline{a} \in G(f(x), p)$, $\underline{b} \in G'(f(x), p)$. Then

- (1) if \underline{a} and \underline{b} are linearly dependent over $\mathbb{Z}/(p)$ with $\underline{a} = \lambda \cdot \underline{b}$, then the set $\{a(t) \mid b(t) = k\}$ is equal to $\{\lambda k\}$,
- (2) if \underline{a} and \underline{b} are linearly independent over $\mathbb{Z}/(p)$, then $\{a(t) \mid b(t) = k\} = \{0, 1, \dots, p-1\}$.

3 Distribution at $\alpha(t) = k$

In this section we always assume p is an odd prime and $e \geq 2$. Let $f(x)$ be a strongly primitive polynomial over $\mathbb{Z}/(p^e)$, $\underline{a}, \underline{b} \in G'(f(x), p^e)$ and $\underline{\alpha} = [h_f(x)\underline{a}_0]_{\text{mod } p}$. Assume $g(x_{e-1}) \in \mathbb{Z}/(p)[x_{e-1}]$ and $\eta_{e-2}(x_0, x_1, \dots, x_{e-2}) \in \mathbb{Z}/(p)[x_0, x_1, \dots, x_{e-1}]$. Let

$$\phi(x_0, x_1, \dots, x_{e-1}) = g(x_{e-1}) + \eta_{e-2}(x_0, x_1, \dots, x_{e-2}).$$

We will prove that for sequences $\underline{a}, \underline{b} \in G'(f(x), p^e)$, $\underline{a} = \underline{b}$ if and only if there exists some $k \in (\mathbb{Z}/(p))^*$ such that the compressing sequences $\phi(a_0(t), a_1(t), \dots, a_{e-1}(t)) = \phi(b_0(t), b_1(t), \dots, b_{e-1}(t))$ at t with $\alpha(t) = k$. We depart the proof into two cases: (1) $\deg g = 1$ and (2) $2 \leq \deg g \leq p-1$.

3.1 Case $\deg g = 1$

When $\deg g = 1$, we can assume $g(x_{e-1}) = x_{e-1}$ without loss of generality. In this case, we do not need $f(x)$ to be a strongly primitive polynomial. In the following, most equalities are regarded as over $\mathbb{Z}/(p)$. we have

Theorem 8. *Let $e \geq 2$ and $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$. Assume $\underline{a}, \underline{b} \in G'(f(x), p^e)$ and*

$$\phi(x_0, x_1, \dots, x_{e-1}) = x_{e-1} + \eta_{e-2}(x_0, x_1, \dots, x_{e-2}),$$

where η_{e-2} is an $(e-1)$ -variable polynomial over $\mathbb{Z}/(p)$. Then $\underline{a} = \underline{b}$ if and only if there exists $k \in (\mathbb{Z}/(p))^$ such that the compressing sequences $\phi(a_0(t), a_1(t), \dots, a_{e-1}(t)) = \phi(b_0(t), b_1(t), \dots, b_{e-1}(t))$ at t with $\alpha(t) = k$.*

Proof. Suppose $\alpha(t) = k \neq 0$, we have

$$a_{e-1}(t) + \eta_{e-2}(a_0(t), \dots, a_{e-2}(t)) = b_{e-1}(t) + \eta_{e-2}(b_0(t), \dots, b_{e-2}(t)). \quad (5)$$

Let $T = p^n - 1$. Then for all $j \geq 0$, $\alpha(t + j \cdot p^{e-2}T) = \alpha(t) = k$. Since $p^{e-2}T$ is a period of $\underline{a}_i, \underline{b}_j$ for $i, j < e-1$, then if we replace t by $j \cdot p^{e-2}T + t$ in (5) and minus it we have

$$a_{e-1}(j \cdot p^{e-2}T + t) - a_{e-1}(t) = b_{e-1}(j \cdot p^{e-2}T + t) - b_{e-1}(t).$$

Let $\underline{\beta} = [h_f(x)\underline{b}_0]_{\text{mod } p}$. By (2) in Proposition 5, we obtain $j \cdot \alpha(t) = j \cdot \beta(t)$ which means that $\beta(t) = k$ when $\alpha(t) = k$. As $\underline{\alpha}, \underline{\beta} \in G'(f(x), p)$, by Proposition 7, we have $\underline{\alpha} = \underline{\beta}$, and then $\underline{a}_0 = \underline{b}_0$.

When $e \geq 4$, the equality (3) in Proposition 5 is just

$$a_{e-1}(j \cdot p^{e-3}T + t) - a_{e-1}(t) = j \cdot (h_f(x)a_1)(t) + C_1(j \cdot (h_{e-2}(x)a_0)(t)) + C_1(a_{e-2}(t) + [j \cdot \alpha(t)]_{\text{mod } p})$$

Since the same equality holds also for $\underline{b_{e-1}}$ and $\underline{a_0} = \underline{b_0}$, we have

$$\begin{aligned} & j \cdot (h_f(x)a_1)(t) + C_1(a_{e-2}(t) + [j \cdot \alpha(t)]_{\text{mod } p}) + \\ & \eta_{e-2}(a_0(t), \dots, a_{e-2}(j \cdot p^{e-3}T + t)) - \eta_{e-2}(a_0(t), \dots, a_{e-2}(t)) = \\ & j \cdot (h_f(x)b_1)(t) + C_1(b_{e-2}(t) + [j \cdot \beta(t)]_{\text{mod } p}) + \\ & \eta_{e-2}(b_0(t), \dots, b_{e-2}(j \cdot p^{e-3}T + t)) - \eta_{e-2}(b_0(t), \dots, b_{e-2}(t)). \end{aligned}$$

As $\underline{a_0} = \underline{b_0}$, by (4), the above equation also holds for $e = 3$. Let $\underline{\tau} = h_f(x)(\underline{a_1} - \underline{b_1})$. From $\alpha(t) = \beta(t) = k$ and replacing e by $e - 1$ in (2), we have

$$\begin{aligned} a_{e-2}(j \cdot p^{e-3}T + t) &= a_{e-2}(t) + j \cdot k, \\ b_{e-2}(j \cdot p^{e-3}T + t) &= b_{e-2}(t) + j \cdot k, \end{aligned}$$

and then

$$\begin{aligned} & j \cdot \tau(t) + C_1(a_{e-2}(t) + [j \cdot k]_{\text{mod } p}) - C_1(b_{e-2}(t) + [j \cdot k]_{\text{mod } p}) = \\ & \eta_{e-2}(b_0(t), \dots, b_{e-2}(t) + j \cdot k) - \eta_{e-2}(b_0(t), \dots, b_{e-2}(t)) - \\ & \eta_{e-2}(a_0(t), \dots, a_{e-2}(t) + j \cdot k) + \eta_{e-2}(a_0(t), \dots, a_{e-2}(t)) \end{aligned}$$

As $k \neq 0$, when j runs over $\{0, 1, \dots, p-1\}$, $[j \cdot k]_{\text{mod } p}$ also runs over $\{0, 1, \dots, p-1\}$. Let $[j \cdot k]_{\text{mod } p} = x$ and then $j = k^{-1}x$. Each side of the above equality can be regarded as a function from $\mathbb{Z}/(p)$ to itself. As such a function can be represented by a polynomial, we denote by $L(x)$ for the left side function and $R(x)$ for the right side. Then we have

$$L(x) = k^{-1}\tau(t)x + C_1(a_{e-2}(t) + x) - C_1(b_{e-2}(t) + x).$$

By Proposition 4, the coefficient of x^{p-1} in $L(x)$ is $-a_{e-2}(t) + b_{e-2}(t)$. Assume

$$\eta_{e-2}(x_0, \dots, x_{e-2}) = -\eta_{e-3}(x_0, \dots, x_{e-3}) \cdot x_{e-2}^{p-1} + \rho_{e-2}(x_0, \dots, x_{e-2}),$$

where the degree of x_{e-2} in $\rho_{e-2}(x_0, \dots, x_{e-2})$ is less than $p-1$. Then the coefficient of x^{e-1} in $R(x)$ is $\eta_{e-3}(a_0(t), \dots, a_{e-3}(t)) - \eta_{e-3}(b_0(t), \dots, b_{e-3}(t))$. Now we have

$$-a_{e-2}(t) + b_{e-2}(t) = \eta_{e-3}(a_0(t), \dots, a_{e-3}(t)) - \eta_{e-3}(b_0(t), \dots, b_{e-3}(t)).$$

and then

$$a_{e-2}(t) + \eta_{e-3}(a_0(t), \dots, a_{e-3}(t)) = b_{e-2}(t) + \eta_{e-3}(b_0(t), \dots, b_{e-3}(t)),$$

which reduce $e - 1$ in (5) to $e - 2$.

By induction, we have that when $\alpha(t) = k$,

$$a_i(t) + \eta_{i-1}(a_0(t), \dots, a_{i-1}(t)) = b_i(t) + \eta_{i-1}(b_0(t), \dots, b_{i-1}(t))$$

holds for $i = 1, 2, \dots, e - 1$, where $\eta_{i-1}(x_0, \dots, x_{i-1})$ is an i -variable polynomial. Let $\underline{c} = \underline{a} - \underline{b}$. For $i = 1$, since $\underline{a}_0 = \underline{b}_0$, we have $\underline{c}_1 \in G(f(x), p)$ and $c_1(t) = a_1(t) - b_1(t) = 0$ whenever $\alpha(t) = k$. Then by Proposition 7, we have $\underline{c}_1 = \underline{0}$, i.e., $[\underline{a}]_{\text{mod } p^2} = [\underline{b}]_{\text{mod } p^2}$. If we have proved that $[\underline{a}]_{\text{mod } p^m} = [\underline{b}]_{\text{mod } p^m}$ for some $m < e$, then we have $\underline{c}_m = \underline{a}_m - \underline{b}_m \in G(f(x), p)$ and $c_m(t) = 0$ whenever $\alpha(t) = k$. Then $\underline{c}_m = \underline{0}$ and $[\underline{a}]_{\text{mod } p^{m+1}} = [\underline{b}]_{\text{mod } p^{m+1}}$. By induction, we can finally prove that $[\underline{a}]_{\text{mod } p^e} = [\underline{b}]_{\text{mod } p^e}$, i.e., $\underline{a} = \underline{b}$. \square

3.2 Case $2 \leq \deg g \leq p - 1$

In this subsection, we will prove the result for $2 \leq \deg g \leq p - 1$. We prove the following lemmas first.

Lemma 9. *Let $f(x)$ be a primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ and $\underline{c} \in G(f(x), p^e)$. Assume $\underline{\gamma} \in G'(f(x), p)$. For $k \in (\mathbb{Z}/(p))^*$, the set $\{c_{e-1}(t) \mid \gamma(t) = k\}$ runs over all elements in $\mathbb{Z}/(p)$ or is a singleton. Moreover, the latter case happens only if $\underline{c}_0 = \dots = \underline{c}_{e-2} = \underline{0}$ and $\underline{c}_{e-1} = \lambda \cdot \underline{\gamma}$, and the singleton is $\{\lambda \cdot k\}$.*

Proof. If $\underline{c}_0 = \dots = \underline{c}_{j-1} = \underline{0}$ and $\underline{c}_j \neq \underline{0}$ with $0 \leq j \leq e - 2$, then $\underline{c} = p^j \underline{c}'$ and $\underline{c}' \in G'(f(x), p^{e-j})$. Since $\underline{c}'_0 \in G'(f(x), p)$, let $h_f(x)$ be defined as in Definition 2 of last section, then $h_f(x) \underline{c}'_0 \in G'(f(x), p)$. By Proposition 7, for some t with $\gamma(t) = k \neq 0$, we have $(h_f(x) \underline{c}'_0)(t) \neq 0$. Replacing e by $e - j$ in equality (2), then $\underline{c}'_{e-j-1}(t)$ can be any element in $\mathbb{Z}/(p)$. As $\underline{c}_{e-1} = \underline{c}'_{e-j-1}$, then \underline{c}_{e-1} can be any element in $\mathbb{Z}/(p)$.

Assume $\underline{c}_0 = \dots = \underline{c}_{e-2} = \underline{0}$. Then $\underline{c}_{e-1} \in G(f(x), p)$. By Proposition 7, if \underline{c}_{e-1} and $\underline{\gamma}$ are linearly independent, then \underline{c}_{e-1} can be any element in $\mathbb{Z}/(p)$. If \underline{c}_{e-1} and $\underline{\gamma}$ are linearly dependent with $\underline{c}_{e-1} = \lambda \cdot \underline{\gamma}$, then it is obvious that the set $\{\underline{c}_{e-1}(t) \mid \gamma(t) = k\}$ is the singleton $\{\lambda \cdot k\}$. \square

Lemma 10. *Let $f(x)$ be a strongly primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with odd prime p and $e \geq 2$. Assume $\underline{a}, \underline{b} \in G'(f(x), p^e)$, $\underline{\alpha} = [h_f(x) \underline{a}_0]_{\text{mod } p}$ and $\underline{\beta} = [h_f(x) \underline{b}_0]_{\text{mod } p}$. Suppose $\underline{\beta} = \lambda \cdot \underline{\alpha}$ holds for some*

$\lambda \in \{1, 2, \dots, p-1\}$. Let $k \in (\mathbb{Z}/(p))^*$. If for those t with $\alpha(t) = k$, the equality

$$b_{e-1}(t) = \delta + \lambda \cdot a_{e-1}(t)$$

always holds, then $\lambda = 1$, $[\underline{a}]_{\text{mod } p^{e-1}} = [\underline{b}]_{\text{mod } p^{e-1}}$ and the sequence $\underline{b_{e-1}} - \underline{a_{e-1}} = \delta k^{-1} \cdot \underline{\alpha}$.

Proof. As $f(x)$ is a strongly primitive polynomial, $\underline{\alpha}$ and $\underline{a_0}$ are linearly independent. By Proposition 7, when $\alpha(t) = k$, $a_0(t)$ can be any element in $\{0, 1, \dots, p-1\}$. Applying the equality (2) for $\underline{a_1}, \dots, \underline{a_{e-1}}$, then when $\alpha(t) = k$, $a(t)$ can be any element in $\{0, 1, \dots, p^e-1\}$.

If $1 \leq \lambda < p-1$, let $\underline{c} = \underline{b} - \lambda \cdot \underline{a} \in G(f(x), p^e)$. Then

$$c_{e-1}(t) = b_{e-1}(t) - \lambda \cdot a_{e-1}(t) - u(t) = \delta - u(t)$$

with $u(t)$ satisfying

$$[b(t)]_{\text{mod } p^{e-1}} + (u(t) - 1)p^{e-1} < \lambda \cdot [a(t)]_{\text{mod } p^{e-1}} \leq [b(t)]_{\text{mod } p^{e-1}} + u(t)p^{e-1}.$$

Since $0 \leq [a(t)]_{\text{mod } p^{e-1}}, [b(t)]_{\text{mod } p^{e-1}} < p^{e-1}$, we have $0 \leq u(t) \leq \lambda$. Since $u(t) \leq \lambda < p-1$, $c_{e-1}(t) = \delta - u(t)$ can not be all elements in $\{0, 1, \dots, p-1\}$. By Lemma 9, $c_{e-1}(t)$ must be a constant when $\alpha(t) = k$. We choose t with $a(t) = 0$, then $u(t) = 0$. When $\lambda \geq 2$, we can also choose t with $\lambda \cdot [a(t)]_{\text{mod } p^{e-1}} > p^{e-1}$, then $u(t) > 0$. So $c_{e-1}(t)$ is not a constant, which is contradiction to Lemma 9. If $\lambda = 1$, then $u(t)$ can only be 0 or 1 and 0 is reachable when $[a(t)]_{\text{mod } p^{e-1}} = 0$. By Lemma 9, we have $u(t)$ can only be 0, and then $\underline{c_0} = \dots = \underline{c_{e-2}} = \underline{0}$ and $c_{e-1}(t) = \delta$ when $\alpha(t) = k$.

If $\lambda = p-1$, let $\underline{c} = \underline{a} + \underline{b} \in G(f(x), p^e)$. Then

$$c_{e-1}(t) = b_{e-1}(t) + a_{e-1}(t) + u(t) = \delta + u(t)$$

with $u(t)$ satisfying

$$u(t) = \begin{cases} 0 & [a(t)]_{\text{mod } p^{e-1}} + [b(t)]_{\text{mod } p^{e-1}} < p^{e-1}, \\ 1 & \text{otherwise.} \end{cases}$$

First we choose $[a(t)]_{\text{mod } p^{e-1}} = 0$. As $[b(t)]_{\text{mod } p^{e-1}} < p^{e-1}$, we have $u(t) = 0$. Then we choose $[a(t)]_{\text{mod } p^{e-1}} = p^{e-1} - 1$, as $\underline{\beta} = \lambda \cdot \underline{\alpha}$ with $\lambda \neq 0$, we have $\underline{b_0} = \lambda \cdot \underline{a_0}$. Then $b_0(t) \neq 0$ and $[a(t)]_{\text{mod } p^{e-1}} + [b(t)]_{\text{mod } p^{e-1}} \geq p^{e-1}$. Thus $u(t) = 1$ and $c_{e-1}(t)$ can only choose 2 elements $\{\delta, \delta + 1\}$, which is contradiction to Lemma 9.

From the above discussion, we have $\lambda = 1$, and then $\underline{c} = \underline{a} - \underline{b}$ and $[\underline{c}]_{p^{e-1}} = \underline{0}$, which means $[\underline{a}]_{\text{mod } p^{e-1}} = [\underline{b}]_{\text{mod } p^{e-1}}$. The statement $c_{e-1}(t) = \delta$ when $\alpha(t) = k$ means $\underline{b_{e-1}} - \underline{a_{e-1}} = \delta k^{-1} \cdot \underline{\alpha}$ by Proposition 7. The proof is complete. \square

Theorem 11. Let $e \geq 2$ and $f(x)$ be a strongly primitive polynomial of degree n over $\mathbb{Z}/(p^e)$. Assume $\underline{a}, \underline{b} \in G'(f(x), p^e)$ and

$$\phi(x_0, x_1, \dots, x_{e-1}) = g(x_{e-1}) + \eta_{e-2}(x_0, x_1, \dots, x_{e-2}),$$

where $2 \leq \deg g \leq p-1$ and η_{e-2} is an $(e-1)$ -variable polynomial over $\mathbb{Z}/(p)$. Then $\underline{a} = \underline{b}$ if and only if there exists some $k \in (\mathbb{Z}/(p))^*$ such that the compressing sequences $\phi(a_0(t), a_1(t), \dots, a_{e-1}(t)) = \phi(b_0(t), b_1(t), \dots, b_{e-1}(t))$ at t with $\alpha(t) = k$.

Proof. Suppose $\alpha(t) = k \neq 0$, we have

$$g(a_{e-1}(t)) + \eta_{e-2}(a_0(t), \dots, a_{e-2}(t)) = g(b_{e-1}(t)) + \eta_{e-2}(b_0(t), \dots, b_{e-2}(t)). \quad (6)$$

Let $T = p^n - 1$. Then for all $j \geq 0$, $\alpha(t + j \cdot p^{e-2}T) = \alpha(t) = k$. Since $p^{e-2}T$ is a period of $\underline{a_i}, \underline{b_j}$ for $i, j < e-1$, then if we replace t by $j \cdot p^{e-2}T + t$ in (6) and minus it we have

$$g(a_{e-1}(j \cdot p^{e-2}T + t)) - g(a_{e-1}(t)) = g(b_{e-1}(j \cdot p^{e-2}T + t)) - g(b_{e-1}(t)). \quad (7)$$

Let $\underline{\beta} = [h_f(x)\underline{b_0}]_{\text{mod } p}$. Again by (2) in Proposition 5, we have

$$a_{e-1}(j \cdot p^{e-2}T + t) = a_{e-1}(t) + j \cdot \alpha(t), \quad (8)$$

$$b_{e-1}(j \cdot p^{e-2}T + t) = b_{e-1}(t) + j \cdot \beta(t). \quad (9)$$

If there exists t such that $\alpha(t) = k$ and $\beta(t) = 0$, substituting the above two equalities to (7) we obtain that

$$g(a_{e-1}(t) + j \cdot k) - g(a_{e-1}(t)) = 0$$

holds for all j . Thus g must be a constant polynomial and it is a contradiction to $2 \leq \deg g \leq p-1$. So when $\alpha(t) = k$, $\beta(t)$ can not be zero. By Proposition 7, we have $\underline{\beta} = \lambda \cdot \underline{\alpha}$ with $\lambda \neq 0$. By (8), we can choose t such that $\alpha(t) = k$ and $a_{e-1}(t) = 0$. If for this t we have $b_{e-1}(t) = \delta$, then from (7), (8) and (9), we have

$$g(j \cdot k) - g(0) = g(\delta + j \cdot \lambda k) - g(\delta).$$

We are going to prove that for t with $\alpha(t) = k$ and $a_{e-1}(t) = 0$, we always have $b_{e-1}(t) = \delta$. If $b_{e-1}(t) = \delta' \neq \delta$, then we also have

$$g(j \cdot k) - g(0) = g(\delta' + j \cdot \lambda k) - g(\delta').$$

From the above two equalities,

$$g(\delta + j \cdot \lambda k) - g(\delta) = g(\delta' + j \cdot \lambda k) - g(\delta').$$

As $j \cdot \lambda k$ runs over all elements in $\mathbb{Z}/(p)$, we have $g(\delta + x) - g(\delta' + x)$ is equal to a constant $g(\delta) - g(\delta')$. Since $\deg g \geq 2$, it is impossible. Then we have proved that for t with $\alpha(t) = k$ and $a_{e-1}(t) = 0$, $b_{e-1}(t)$ is equal to δ . From $\underline{\beta} = \lambda \cdot \underline{\alpha}$ and equalities (8) and (9), we have for t with $\alpha(t) = k$ and $a_{e-1}(t) = 0$,

$$b_{e-1}(j \cdot p^{e-2}T + t) = \delta + \lambda \cdot a_{e-1}(j \cdot p^{e-2}T + t).$$

The above equality holds for all $j \geq 0$. Then for t_0 with $\alpha(t_0) = k$, there exists some $0 \leq j_0 \leq p-1$ such that $a_{e-1}(j_0 \cdot p^{e-2}T + t_0) = 0$. The above equation holds for $t = j_0 \cdot p^{e-2}T + t_0$ and $j = p - j_0$. then

$$\begin{aligned} b_{e-1}(t_0) &= b_{e-1}(p^{e-1}T + t_0) = b_{e-1}(j \cdot p^{e-2}T + t) \\ &= \delta + \lambda \cdot a_{e-1}(j \cdot p^{e-2}T + t) \\ &= \delta + \lambda \cdot a_{e-1}(p^{e-1}T + t_0) \\ &= \delta + \lambda \cdot a_{e-1}(t_0). \end{aligned}$$

We have proved that for t with $\alpha(t) = k$, $b_{e-1}(t) = \delta + \lambda \cdot a_{e-1}(t)$ always holds. By Lemma 10, we have

$$\lambda = 1, \quad [\underline{a}]_{\text{mod } p^{e-1}} = [\underline{b}]_{\text{mod } p^{e-1}}, \quad \underline{b_{e-1}} = \underline{a_{e-1}} + \delta.$$

Now we go back to equality (6). Since when $\alpha(t) = k$, $a_{e-1}(t)$ can be any element in $\{0, 1, \dots, p-1\}$, then we have $g(x) = g(x + \delta)$. As $2 \leq \deg g \leq p-1$, we must have $\delta = 0$. Thus $\underline{b_{e-1}} = \underline{a_{e-1}}$ and we have proved that $[\underline{a}]_{\text{mod } p^{e-1}} = [\underline{b}]_{\text{mod } p^{e-1}}$. So $\underline{a} = \underline{b}$, and the proof is complete. \square

From Theorem 8 and Theorem 11, we have proved what we state at the beginning of this section.

4 s -uniform

Let $f(x)$ be a strongly primitive polynomial of degree n over $\mathbb{Z}/(p^e)$ with odd prime p and $e \geq 2$. Assume $\underline{a}, \underline{b} \in G'(f(x), p^e)$. Let

$$\phi(x_0, x_1, \dots, x_{e-1}) = g(x_{e-1}) + \eta_{e-2}(x_0, x_1, \dots, x_{e-2})$$

with η_{e-2} an $(e-1)$ -variable polynomial over $\mathbb{Z}/(p)$. In Theorem 3 [13, Theorem 9], Zheng, Qi and Tian prove that when $g(x_{e-1}) = x_{e-1}$ and the coefficient of $x_{e-2}^{p-1} \cdots x_1^{p-1} x_0^{p-1}$ in η_{e-2} is not equal to $(-1)^e \cdot \frac{p+1}{2}$, then $\underline{a} = \underline{b}$ if and only if there exist $s \in \mathbb{Z}/(p)$ and $k \in (\mathbb{Z}/(p))^*$ such that $\phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1})$ and $\phi(\underline{b}_0, \underline{b}_1, \dots, \underline{b}_{e-1})$ are s -uniform with $\underline{a}|_k$. In this section, we will discuss the s -uniform property for general $g(x_{e-1})$.

If the image of polynomial ϕ is not $\mathbb{Z}/(p)$, i.e., there is some s in $\mathbb{Z}/(p)$ such that $\phi(x_0, x_1, \dots, x_{e-1}) \neq s$ for all e -tuples in $(\mathbb{Z}/(p))^e$, then it is obvious that for any \underline{a} and \underline{b} , $\phi(a_0(t), a_1(t), \dots, a_{e-1}(t)) = s$ if and only if $\phi(b_0(t), b_1(t), \dots, b_{e-1}(t)) = s$. Thus we only consider the case that s is an image of ϕ . Since when $\alpha(t) = k$, $a(t)$ can be any element in $\{0, 1, \dots, p^e - 1\}$ by the proof of Lemma 10, s is an image of ϕ if and only if there is some t with $\alpha(t) = k$ such that $\phi(a_0(t), a_1(t), \dots, a_{e-1}(t)) = s$.

We first consider the case that $g(x_{e-1})$ is a permutation polynomial. We define a function $\psi_{z,w}$ from $(\mathbb{Z}/(p))^{e-1}$ to $\mathbb{Z}/(p)$ by

$$\psi_{z,w}(x_0, \dots, x_{e-2}) = \begin{cases} z, & \text{if } (x_0, \dots, x_{e-2}) = (0, \dots, 0), \\ w, & \text{if } (x_0, \dots, x_{e-2}) \neq (0, \dots, 0). \end{cases}$$

The polynomial representation of $\psi_{z,w}$ is

$$\psi_{z,w}(x_0, \dots, x_{e-2}) = (z - w)(1 - x_0^{p-1}) \cdots (1 - x_{e-2}^{p-1}) + w.$$

We have the following theorem.

Theorem 12. *Let $\underline{a}, \underline{b} \in G'(f(x), p^e)$ and $\underline{b} = -\underline{a}$. Assume*

$$\phi(x_0, \dots, x_{e-1}) = g(x_{e-1}) + \psi_{z,w}(x_0, \dots, x_{e-2})$$

with $g(x_{e-1})$ a permutation polynomial. Then, for any s in $\mathbb{Z}/(p)$, we can choose suitable z and w such that $\phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1})$ and $\phi(\underline{b}_0, \underline{b}_1, \dots, \underline{b}_{e-1})$ are s -uniform.

Proof. We solve the equations

$$\begin{cases} g(\frac{p-1}{2}) + w = s \\ g(0) + z = s \end{cases}$$

to get the unique z and w . As $g(x_{e-1})$ is a permutation polynomial and $\psi_{z,w}$ is a two-value function. $\phi(x_0, \dots, x_{e-1}) = s$ if and only if the following two cases happen

$$\begin{aligned} g(x_{e-1}) = s - z & \quad \psi_{z,w}(x_0, \dots, x_{e-2}) = z, \\ g(x_{e-1}) = s - w & \quad \psi_{z,w}(x_0, \dots, x_{e-2}) = w. \end{aligned}$$

If and only if $(x_0, \dots, x_{e-2}, x_{e-1})$ satisfies one of the following two conditions

$$\begin{aligned} (x_0, \dots, x_{e-2}) &= (0, \dots, 0) & x_{e-1} &= 0, \\ (x_0, \dots, x_{e-2}) &\neq (0, \dots, 0) & x_{e-1} &= \frac{p-1}{2}. \end{aligned} \quad (*)$$

When $\underline{b} = -\underline{a}$, the e -tuple $(a_0(t), \dots, a_{e-2}(t), a_{e-1}(t))$ satisfies $(*)$ if and only if $(b_0(t), \dots, b_{e-2}(t), b_{e-1}(t))$ satisfies $(*)$. Then for time t , we have $\phi(a_0(t), a_1(t), \dots, a_{e-1}(t)) = s$ if and only if $\phi(b_0(t), b_1(t), \dots, b_{e-1}(t)) = s$, i.e., $\phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1})$ and $\phi(\underline{b}_0, \underline{b}_1, \dots, \underline{b}_{e-1})$ are s -uniform. \square

Remark 1. In [13, Theorem 21], Zheng, Qi and Tian give a counterexample of Theorem 3, if the condition that the coefficient of $x_{e-2}^{p-1} \cdots x_1^{p-1} x_0^{p-1}$ in η_{e-2} is equal to $(-1)^e \cdot \frac{p+1}{2}$. Their result is when

$$\phi(x_0, \dots, x_{e-1}) = x_{e-1} + (-1)^e (x_{e-2}^{p-1} - 1) \cdots (x_0^{p-1} - 1) - \frac{p-1}{2},$$

for $\underline{b} = -\underline{a}$, the corresponding compressing sequences are 0-uniform. If we let $g(x_{e-1}) = x_{e-1}$ and $s = 0$ in the above theorem, then $z = 0$ and $w = \frac{p+1}{2}$. From the polynomial representation of $\psi_{z,w}$, our result coincides with their's.

When $g(x_{e-1})$ is not a permutation polynomial and satisfies an additional condition in the following theorem, there exist many choices of η_{e-2} such that for different $\underline{a}, \underline{b} \in G'(f(x), p^e)$, $\phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1})$ and $\phi(\underline{b}_0, \underline{b}_1, \dots, \underline{b}_{e-1})$ are s -uniform. For a nonempty subset W of $\{0, 1, \dots, p-1\}$, we use $\psi_{z,W}$ to denote any function from $(\mathbb{Z}/(p))^{e-1}$ to $\mathbb{Z}/(p)$ satisfying

$$\psi_{z,W}(x_0, \dots, x_{e-2}) = \begin{cases} z, & \text{if } (x_0, \dots, x_{e-2}) = (0, \dots, 0), \\ w \in W, & \text{if } (x_0, \dots, x_{e-2}) \neq (0, \dots, 0). \end{cases}$$

Given s and W , when W is a singleton $\{w\}$, $\psi_{z,W}$ is uniquely determined and equal to $\psi_{z,w}$. But when W has more than one element, there exist many such $\psi_{z,W}$, especially when the cardinality of W is large.

Theorem 13. Assume $g(x_{e-1})$ satisfies

- (1) it is not a permutation polynomial, i.e., the image set I of $g(x_{e-1})$ is a proper subset of $\{0, 1, \dots, p-1\}$,
- (2) for some $r \in I$, there exists $\lambda \neq 0, 1$, for $y \in \mathbb{Z}/(p)$, such that $g(y) = r$ if and only if $g(\lambda \cdot y) = r$.

For an element s in $\mathbb{Z}/(p)$, let W be the nonempty set $\{w \mid s \notin w + I\}$, and

$$\phi(x_0, \dots, x_{e-1}) = g(x_{e-1}) + \psi_{z,W}(x_0, \dots, x_{e-2}).$$

Then we can choose suitable z such that for $\underline{a}, \underline{b} \in G'((x), p^e)$ with $\underline{b} = \lambda \cdot \underline{a}$, $\phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1})$ and $\phi(\underline{b}_0, \underline{b}_1, \dots, \underline{b}_{e-1})$ are s -uniform.

Proof. Let $z = s - r$. According to the definition of W , for each $w \in W$ and $i \in I$, we have $w + i \neq s$. Thus if $\phi(x_0, \dots, x_{e-1}) = s$, then $(x_0, \dots, x_{e-2}, x_{e-1}) = (0, \dots, 0, y)$ with $g(y) = r$. By condition (2), $g(y) = r$ if and only if $g(\lambda \cdot y) = r$. Thus when $\underline{b} = \lambda \cdot \underline{a}$, $\phi(a_0(t), a_1(t), \dots, a_{e-1}(t)) = s$ if and only if $\phi(b_0(t), b_1(t), \dots, b_{e-1}(t)) = s$. So they are s -uniform. \square

We give an example of $g(x_{e-1})$ which satisfies the two conditions in the above theorem.

Corollary 14. *Assume $g(x_{e-1})$ is not a permutation and $g(y) = g(0)$ if and only if $y = 0$. For given s in $\mathbb{Z}/(p)$, let ϕ defined as in the above theorem. Then for $\underline{a}, \underline{b} \in G'(f(x), p^e)$ with $\underline{b} = \lambda \cdot \underline{a}$, $\phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1})$ and $\phi(\underline{b}_0, \underline{b}_1, \dots, \underline{b}_{e-1})$ are s -uniform.*

Proof. As the preimage of $g(0)$ is 0. For any $\lambda \neq 0$, the condition (2) in the above theorem is satisfied. The result follows from the above theorem. \square

We discuss for a certain $\phi(x_0, \dots, x_{e-1})$ and different $\underline{a}, \underline{b} \in G'(f(x), p^e)$, $\phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1})$ and $\phi(\underline{b}_0, \underline{b}_1, \dots, \underline{b}_{e-1})$ can be s -uniform for how many s . The following lemma about the sum of Legendre symbols can be found in [4, Chapter 5].

Lemma 15. *For an odd prime p , we have*

$$\sum_{x=0}^{p-1} \left(\frac{x^2 + w}{p} \right) = \begin{cases} p-1, & \text{if } p \mid w, \\ -1, & \text{if } p \nmid w. \end{cases}$$

Theorem 16. *Let $g(x_{e-1}) = x_{e-1}^2$. Assume*

$$\phi(x_0, \dots, x_{e-1}) = g(x_{e-1}) + \psi_{0,w}(x_0, \dots, x_{e-2}).$$

Then for $\underline{a}, \underline{b} \in G'(f(x), p^e)$ with $\underline{b} = -\underline{a}$, and suitable w , there are $\lfloor \frac{p}{4} \rfloor + 1$ elements s such that $\phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1})$ and $\phi(\underline{b}_0, \underline{b}_1, \dots, \underline{b}_{e-1})$ are s -uniform.

Proof. Let I denote the image set of x_{e-1}^2 , i.e., $I = \{x^2 \mid x \in \mathbb{Z}/(p)\}$, and $I_w = w + I = \{w + x^2 \mid x \in \mathbb{Z}/(p)\}$. Then $|I| = |I_w| = \frac{p+1}{2}$. As for each $r \in I$, $y^2 = r$ if and only if $(-y)^2 = r$. By theorem 13, we have that for each $s \in I \setminus I_w$, $\phi(\underline{a}_0, \underline{a}_1, \dots, \underline{a}_{e-1})$ and $\phi(\underline{b}_0, \underline{b}_1, \dots, \underline{b}_{e-1})$ are s -uniform.

Now we count the number of elements in $I \cap I_w$ with $w \neq 0$. We calculate the sum $1 + \left(\frac{w+x^2}{p} \right)$ over all $x \in \mathbb{Z}/(p)$. Let $y = w + x^2$. If $x \neq 0$ and $y \in I \setminus \{0\}$, the element y is counted 4 times. If $x = 0$ and $y \in I$, y is

counted 2 times. If $y = 0$, then y is counted 2 times. By the above lemma, then

$$\begin{aligned} |I \cap I_w| &= \frac{1}{4} \sum_{x \in \mathbb{Z}/(p)} \left(1 + \left(\frac{w+x^2}{p}\right)\right) + \frac{1 + \left(\frac{w}{p}\right)}{4} + \frac{1 + \left(\frac{-w}{p}\right)}{4} \\ &= \frac{p-1}{4} + \frac{2 + \left(\frac{w}{p}\right) + \left(\frac{-w}{p}\right)}{4} \\ &= \frac{p+1 + \left(\frac{w}{p}\right) + \left(\frac{-w}{p}\right)}{4} \end{aligned}$$

If $p \equiv 3 \pmod{4}$, then $\left(\frac{w}{p}\right) + \left(\frac{-w}{p}\right) = 0$. We have $|I \cap I_w| = \frac{p+1}{4}$ and then $|I \setminus I_w| = \frac{p+1}{4} = \left[\frac{p}{4}\right] + 1$.

If $p \equiv 1 \pmod{4}$, choose w such that $\left(\frac{w}{p}\right) = \left(\frac{-w}{p}\right) = -1$. Then $|I \cap I_w| = \frac{p-1}{4}$. Thus $|I \setminus I_w| = \frac{p+3}{4} = \left[\frac{p}{4}\right] + 1$. The proof is complete. \square

5 Conclusions

In this article, we consider the distribution properties of compressing sequences derived from primitive sequences modulo odd prime powers. For strongly primitive polynomial $f(x)$ and compressing map

$$\phi(x_0, x_1, \dots, x_{e-1}) = g(x_{e-1}) + \eta_{e-2}(x_0, x_1, \dots, x_{e-2})$$

with $1 \leq \deg g \leq p-1$, primitive sequences $\underline{a} = \underline{b}$ if and only if the compressing sequences $\phi(a_0(t), \dots, a_{e-1}(t)) = \phi(b_0(t), \dots, b_{e-1}(t))$ for all the t with $\alpha(t) = k$. When $\deg g = 1$, we do not need $f(x)$ to be a strongly primitive polynomial. This result improves the result in [10, Theorem 5]. For s -uniform property, when $g(x_{e-1})$ is a permutation polynomial, for a certain $\phi(x_0, \dots, x_{e-1})$, the compressing sequences of \underline{a} and $-\underline{a}$ are s -uniform. When $g(x_{e-1})$ is not a permutation polynomial, there may exist many $\phi(x_0, \dots, x_{e-1})$ such that the compressing sequences of \underline{a} and $\lambda \cdot \underline{a}$ are s -uniform. For $g(x_{e-1}) = x_{e-1}^2$, we can construct a compressing map $\phi(x_0, \dots, x_{e-1})$ such that the compressing sequences of \underline{a} and $-\underline{a}$ are s -uniform for $\left[\frac{p}{4}\right] + 1$ different s in the image of ϕ .

References

- [1] Zong-Duo Dai, Binary sequences derived from ML-sequences over rings I: Periods and minimal polynomials, *J. Crypt.*, 1992, **5**(3), 193–207.

- [2] Z. D. Dai, T. Beth and D. Gollmann, Lower bounds for the linear complexity of sequences over residue rings, *EUROCRYPT'90*, LNCS 473, 189–195.
- [3] Minqiang Huang and Zongduo Dai, Projective maps of linear recurring sequences with maximal p -adic periods, *Fibonacci Quart.*, 1992, **30**(2), 139–143.
- [4] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag New York, 1990.
- [5] V. L. Kurakin, A. S. Kuzmin, A. V. Mikhalev and A. A. Nechaev, Linear recurring sequences over rings and modules, *J. Math. Sci.* 1995, **76**(6), 2793–2915.
- [6] A. S. Kuzmin, Lower estimates for the ranks of coordinate sequences of linear recurrent sequences over primary residue rings of integers, *Russ. Math. Surv.*, 1993, **48**(3), 203–204.
- [7] A. S. Kuzmin and A. A. Nechaev, Construction of noise-resistant codes by means of linear recurrences over Galois rings, *Russ. Math. Surv.*, 1992, **47**(5), 189–190.
- [8] A. S. Kuzmin and A. A. Nechaev, Linear recursive sequences over Galois rings, *Russ. Math. Surv.*, 1993, **48**(1), 171–172.
- [9] W. F. Qi, J. H. Yang and J. J. Zhou, ML-sequences over rings $\mathbb{Z}/(2^e)$: I. constructions of nondegenerative ML-sequences II. injectivness of compression mappings of new classes, *ASIACRYPT'98*, LNCS 1514, 315–326.
- [10] T. Tian and W. F. Qi, Injectivity of compressing maps on primitive sequences over $\mathbb{Z}/(p^e)$, *IEEE Trans. Inf. Theory*, 2007, **53**(8), 2960–2966.
- [11] M. Ward, The arithmetical theory of linear recurring series, *Trans. Amer. Math. Soc.*, 1933, **35**(3), 600–628.
- [12] Q. X. Zheng and W. F. Qi, Distribution properties of compressing sequences derived from primitive sequences over $\mathbb{Z}/(p^e)$, *IEEE Trans. Inf. Theory*, 2010, **56**(1), 555–563.
- [13] Q. X. Zheng, W. F. Qi and T. Tian, Further result on distribution properties of compressing sequences derived from primitive sequences over $\mathbb{Z}/(p^e)$, *IEEE Trans. Inf. Theory*, 2013, **59**(8), 5016–5022.

- [14] X. Y. Zhu and W. F. Qi, Compression mappings on primitive sequences over $\mathbb{Z}/(p^e)$, *IEEE Trans. Inf. Theory*, 2004, **50**(10), 2442–2448.
- [15] X. Y. Zhu and W. F. Qi, Uniqueness of the distribution of zeros of primitive level sequences over $\mathbb{Z}/(p^e)$, *Finite Fields Appl.*, 2005, **11**(1), 30–44.
- [16] X. Y. Zhu and W. F. Qi, Uniqueness of the distribution of zeros of primitive level sequences over $\mathbb{Z}/(p^e)$ (II), *Finite Fields Appl.*, 2007, **13**(2), 230–248.
- [17] X. Y. Zhu and W. F. Qi, Further result on compressing maps on primitive sequences modulo odd prime powers, *IEEE Trans. Inf. Theory*, 2007, **53**(8), 2985–2990.
- [18] X. Y. Zhu and W. F. Qi, On the distinctness of modular reductions of maximal length sequences modulo odd prime powers, *Math. Comput.*, 2008, **77**(263), 1623–1637.